HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128

DIRECTIVE
NUMBER 100-8 26 March 1999

COMMUNICATIONS-ELECTRONICS

Theater Policy for the
Defense Information System Network

---

1. **Summary**. This directive establishes US European Command (USEUCOM) policy and prescribes responsibilities for operation and use of the Defense Information Systems Network (DISN), its legacy and successor systems. It details policy for management, use, and access to these networks and connected services.

2. **Applicability**. This directive applies to all HQ USEUCOM directorates/staff offices, DOD components, and associated agencies operating in the USEUCOM area of responsibility (AOR).

3. **Internal Control Systems**. This directive contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. The proponent for this directive is the Defense-Wide Systems Division, Command, Control and Communications Systems Directorate, HQ USEUCOM. Address suggested improvements to: HQ USEUCOM/ECJ6-SS, Unit 30400, Box 1000, APO AE 09128.

5. **References**. (See Appendix A).

6. **Definitions**. (See Appendix B, part II).

7. **Policy**.

a. **General.**

(1) The DISN is the primary integrated command and control network for voice, data, video teleconferencing (VTC), and messaging services for USEUCOM and its components.

This Directive supersedes ED 100-8, dated 6 Feb 90.

(2) All DOD long-haul communications requirements for the USEUCOM AOR will be submitted to DISA-EUR. DISA-EUR will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements within theater. Existing component networks that duplicate DISN services will be identified to the appropriate theater configuration control board (TCCB) and be reviewed on an annual basis for possible DISN migration based on interoperability, network integrity and control combined with enterprise-level cost optimization.

b. **Connection to the DISN.**

(1) All connections to the DISN-Europe require DISA-EUR technical approval after operational requirements validation by USEUCOM ECJ6 or the component command as appropriate.

(2) Connections to the DISN by non-DOD, allied, or foreign agencies or activities will be validated by ECJ6 prior to connection.

(3) All proposed changes to the configuration of the DISN infrastructure (backbone) will be submitted to the appropriate TCCB for approval prior to implementation in accordance with ref. I, pg. A-1.

(4) Component commanders have validation authority for communications networks within the boundaries of local base, post, camp or station. For the purpose of this policy, a cluster of facilities within geographic proximity to one another comprise a base, post, camp or station. These clusters must be defined and approved by USEUCOM ECJ6.

(5) Components and agencies will not plan to field communications equipment that does not have Host Nation Approval (HNA) for the country of intended use. HNA will be obtained before equipment is nominated to fill a requirement in a technical solution.

(6) Components and agencies will not plan to field communications equipment that does not have Connection Approval (CA) for the country of intended use. CA will be obtained before equipment is nominated to fill a requirement in a technical solution. Normally the manufacturer or supplier of the equipment will be required to obtain the CA in the acquisition document. However, if this is not the case, the Program Manager (PM) for the implementation is required to specifically appoint someone to obtain the requisite approval following the guidance in ref. L, pg. A-1.

c. **Use of the DISN.**

(1) The DISN is for official business and authorized purposes only. The DISN is the primary network for voice, data, video teleconferencing (VTC), and messaging services for USEUCOM and its components. Use of the DISN constitutes consent to have communications monitored for security and management purposes.

(2) DISN-Europe will not be used as a parallel network or alternate route for non-DOD or allied systems or networks. See ref. F, pg. A-1.

(3) Toll-skipping at a DISN voice or data switch/gateway (e.g. automatic interconnection between incoming long-distance DSN calls and the local commercial system) will not be allowed. See ref. E, pg. A-1.

(4) Use of the DISN to support health, morale and welfare is permitted as an important means of enhancing morale. Off-netting at a DISN voice or data switch/gateway (e.g. connecting service member callers to an off-base number) will not incur a toll cost to DOD. Off-netting within the authorized local commercial calling area of the DISN switch will not be treated as a toll call. For off-netting beyond the local commercial calling area of the DISN switch, local commanders will establish policy and procedures to ensure calls are made collect or to toll-free numbers; or if charges are incurred, they are billed to a non-government telephone number, a personal telephone credit card, or will be reimbursed to DOD in accordance with established collection procedures. USEUCOM encourages base, post, camp, and station commanders to support this program by providing training and instructions to switchboard operators on implementing this policy. See Appendix G for additional information concerning health, morale, and welfare policy.

(5) Within Europe, the European DISN Video Services - Global (DVS-G) hub will be used by all DOD and federal agencies. The DVS-G hub will be the primary multi-point control unit for all non-tactical VTC users.

8. **Responsibilities - HQ USEUCOM**

a. The Director, Command, Control, and Communications Directorate, ECJ6, exercises supervision of the DISN European segment and is responsible for establishing policy, restoration priorities, validating system architectures, connection, and access requirements for any application or system using the electromagnetic spectrum and/or requiring long-haul common-user information transfer services within USEUCOM. ECJ6 may delegate validation authority for special circuits and sub-networks to the appropriate USEUCOM staff element or component command. JWICS validation is delegated to ECJ2. In addition ECJ6 will:

(1) Forward validated requirements to DISA-EUR for security, technical, and interoperability approval. If required, ECJ6 will submit the requirement to the appropriate Designated Approval Authority (DAA) for review/approval. USEUCOM will forward requirements requiring JCS approval as appropriate. (See Appendix H)

(2) Review service restoration priority requests in accordance with National Security and Emergency Preparedness (NS/EP) and Telecommunications Service Priority (TSP) procedures.

(3) Provide a member to the DISN-Europe Configuration Management Board and the TCCBs for voice, data, and transmission.

(4) Implement, enforce, and comply with policies and procedures in references A through L, pg. A-1.

(5) Serve as the USEUCOM interface to DISA-EUR.

(6) Reconcile requirements conflicts.

(7) Process HNA requests from DISN program managers and components.

b. USEUCOM Inspector General, ECIG, will ensure Inspector General team surveys and reports include analysis of user telecommunications economy and discipline IAW ref. G, pg. A-1.

9. **Responsibilities - Defense Information Systems Agency (DISA).** DISA defines the security, technical, interoperability, and performance standards for the entire DISN. DISA-EUR, as the field operating agency for DISA in the USEUCOM AOR, serves as the theater single system network manager of the DISN. DISA-EUR responsibility includes network monitoring and control of theater-wide DISN access points, DISN networks and backbone services such as: DSN, DRSN, NIPR, SIPR, DSCS, BC2A, DEB, ATM, and STEP. DISA-EUR will:

a. Approve all security, technical, and interoperability specifications for applications requiring DISN long-haul common-user information transfer services. Based on direction and guidance from HQ DISA, DISA-EUR will ensure all systems/solutions comply with the current Joint Technical Architecture.

b. Establish procedures for and chair the DISN-Europe configuration management board and the theater configuration control boards for voice, data, and transmission. Procedures will include board composition, meeting frequency and method, and the definition and dissemination of the configuration control process.

c. Provide operational management of the DISN and implement solutions to requirements validated by USEUCOM.

d. Provide USEUCOM ECJ6 reports on network performance and usage as required.

e. Implement and comply with policies and procedures in references A through L.

10. **Responsibilities - Other**. USEUCOM component commands, DOD agencies, services and their elements operating in USEUCOM are responsible for efficient operations, maintenance, and funding of the deployed block and designated portions of the sustaining block of the DISN such as user data terminal equipment, telephones, facsimile machines, computers, video teleconference suites, premise routers, base outside plant, etc. They are responsible for ensuring that their portions of the DISN conform to security, technical, interoperability, and performance standards established by DISA. In addition:

a. Components and agencies fielding communications systems and/or computer networks will ensure these systems comply with the current Joint Technical Architecture or its successors. They will also ensure all necessary Host Nation Approvals and Connection Approvals have been obtained prior to fielding systems in this theater.

b. Components and agencies will not develop or field communications and computer networks or systems that duplicate Defense Information Systems Agency (DISA) provided services, or fail to meet DISA technical specifications, interoperability, security, and performance requirements.

Agencies and elements of different components within the same metropolitan area will share DISN resources, switches, routers, etc. to the maximum extent.

c. Components and agencies will ensure that internet protocol (IP) capable systems use NIPRNET, SIPRNET, or JWICS services unless waivered. Interoperability, timeliness of services, network integrity/control, combined with enterprise-level cost optimization shall form the basis for the waiver process.

d. Components will forward requirements for use of the electromagnetic spectrum, DISN access or service by non-DOD agencies or foreign governments to HQ USEUCOM ECJ6 for validation and/or approval.

e. Components will forward requirements for DSN and DRSN precedence above the ROUTINE level to ECJ6 for validation and or approval IAW ref. C, pg. A-1 (see Appendix D).

f. Components will establish audit procedures for DISN provided services and review requirements on a biennial basis. Services no longer required will be canceled.

g. Components will validate access and connection requirements for applications and systems at the individual local base, post, camp, or station.

h. Components and agencies will ensure Inspector General team surveys and reports include analysis of use of DISN services for economy and discipline.

i. Components and agencies will appoint members to the DISN-Europe Configuration Management Board and TCCBs for voice, data, and transmission IAW ref. I, pg. A-1.

j. Components and agencies will implement and comply with policies and procedures in this directive and references A through L.

k. Components will operate their portions of the DISN in compliance with DISA network management procedures.

l. Components and agencies will avoid dedicated point-to-point DISN services where practical.

m. Components headquarters shall validate all urgent telecommunications requirements with ECJ6-S prior to submission of an urgent Request for Service (RFS). Validation for urgent RFSs at component headquarters must be accomplished at the O-6/GS civilian equivalent level.

11. **Summary of Changes**. This directive:

a. Replaces ED 100-8, Theater Policy for Communications Service to Morale, Welfare, and Recreation (MWR) Activities, 6 February 1990, incorporating previous MWR communications support policy into this document.

b. Incorporates USEUCOM implementing policy and guidance for CJCSIs 6115.01, 6211.02A, 6215.01, 6740.01, and 6900.01 into a single policy document.

c. Establishes requirement for HNA and CA to be obtained before equipment is nominated as a technical solution to fill a requirement.

d. Establishes the DISN as the primary DOD long-haul command and control telecommunications network for USEUCOM.

e. Incorporates DISA-EUR policy for configuration management of the DISN.

f. Establishes policy and responsibilities for DISN management, use, and access.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

MICHAEL A. CANAVAN
Lieutenant General, USA
Chief of Staff

SUSAN M. MEYER
LTC, USA
Adjutant General

APPENDIXES:

A - References
B - Definitions
C - Allied/Foreign Access
D - Defense Switched Network/Defense Red Switch Network
E - Video-Teleconference Networks
F - Data Networks
G - Health, Morale and Welfare use of the DISN
H - DISN Requirements Validation Procedures
I - DISN-Europe Configuration Management Policy

DISTRIBUTION:
P

APPENDIX A
References

A. CJCSI 5721.01, 28 June 1993, “Defense Message System Network and Connected Systems.”

B. CJCSI 6115.01, 23 Oct 95, “Reduction, Realignment, and Contracting of Command, Control, Communications and Computer Facilities.”

C. CJCSI 6211.02A, 22 May 96, “Defense Information System Network and Connected Systems.”

D. CJCSI 6212.01, 30 Jul 93 “Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems.”

E. CJCSI 6215.01, 1 Feb 95, “Policy for the Defense Switched Network.”

F. CJCSI 6740.01, 1 Sep 96, “Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations.”

G. CJCSI 6900.01, 24 Dec 96, “Telecommunications Economy and Discipline.”

H. Memorandum Of Understanding (MOU), 15 Apr 95, between USCINCEUR and Director, Defense Information Systems Agency (DISA).

I. DISAEI 300-50-1, 15 Apr 98, DISA-Europe Policy for Implementing Configuration Management within the Defense Information System Network-Europe (DISN-E).

J. Department of Defense (DOD) 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993 (w/ch2).

K. DISA -Circular 310-130-1 and DISA-EUR Sup 1, “Submission of Telecommunications Requests.”

L. DISA-EUR-Circular 310-140-2, “Leased Services and Facilities Connection Approval Procedures.”

APPENDIX B

GLOSSARY

Part I – Abbreviations and Acronyms

AOR	Area of Responsibility
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AUTODIN	Automatic Digital Network
CINC	Commander of a Unified Command
CA	Connection Approval
C2	Command and Control
C3	Command, Control, and Communications
C4I	Command, Control, Communications, Computers, and Intelligence
CCB	Configuration Control Board
CCSD	Command Communications Service Designator
CISA	C4I Integration Support Activity
COMPUSEC	Computer Security
COMSEC	Communications Security
CONUS	Continental United States
CUDN	Common User Data Network
DAA	Designated Approval Authority
DeCA	Defense Commissary Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DODEA	Department of Defense Education Activity

DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVS-G	DISN Video Services - Global
DWCF	Defense Working Capital Fund
EAC	Emergency Action Console
EO	End Office
FMS	Foreign Military Sales
GOS	Grade of Service
HMW	Health, Morale, and Welfare
HNA	Host Nation Approval
IDNX	Integrated Data Network Exchange
ISDN	Integrated Service Digital Network
IST	Inter-Switch Trunks
IVSN	Initial Voice Switched Network
JWICS	Joint Worldwide Intelligence Communication System
MCA	Metropolitan Calling Area
MFS	Multifunction Switch
MLPP	Multilevel Precedence and Preemption
MTF	Message Text Format
NACSI	National Communications Security Instructions
NAF	Non-Appropriated Fund
NATO	North Atlantic Treaty Organization
NIPRNET	Unclassified Internet Protocol Router Network
NM	Network Management
NSA	National Security Agency

NS/EP	National Security and Emergency Preparedness
O&M	Operation and Maintenance
OCONUS	Outside CONUS
PANS	Private-Accessed Network System
PBX	Private Branch Exchange
POTS	Plain Old Telephone Service
PTT	Public Telephone and Telegraph
RMC	Resource Management Committee (CISA)
SCI	Sensitive Compartmented Information
SDN	Secure Data Network
SIPRNET	Secret Internet Protocol Router Network
STU-III	Secure Telephone Unit Three/Low-Cost Terminal
TCCB	Theater Configuration Control Board
TSP	Telecommunications Service Priority System
USAFE	United States Air Forces in Europe
USAREUR	United States Army, Europe
USMARFOREUR	United States Marine Forces, Europe
USNAVEUR	United States Naval Force, Europe
VTC	Video Teleconferencing

Part II -- Definitions

Avoidance Routing - Circuits routed so as to avoid critical junctions and known target areas.

Backbone - The DISN backbone consists of nodal switches, connectivity among nodals, long-distance termination at DSN EOs, connectivity between EOs and nodal switches, and connectivity between EOs.

Commander in Chief (CINC) - Commander of one of the following unified commands: US Atlantic Command, US Central Command, US European Command, US Pacific Command, US Southern Command, US Space Command, US Special Operations Command, US Strategic Command, US Transportation Command.

Command and Control (C2)- The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JCS Pub 1-02)

Connection Approval (CA) - A commercial approval to connect C4 equipment that is capable of interacting with the host nation's commercial public telephone and telegraph (PTT) network or public telecommunications network (PTN). Within the European Community (EC), CA is required if equipment is capable of inter-working with a public network, regardless of whether the equipment is connected directly, indirectly or not at all. Inter-working is defined as being capable of establishing, modifying, charging, holding and clearing, a real or virtual connection. This includes leased point to point circuits as well.

C2 Users - Users who have a requirement for C2 communications but do not meet the criteria for the class of "special C2 user." C2 users include any person (regardless of the position in the chain-of-command) who issues guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration and logistics), whether said guidance or order is issued or effected during peace or wartime. C2 users are identified as users of Joint Staff, CINC-, Service-, and agency-approved PRIORITY and ROUTINE precedence origination capability.

C4 Systems Operational Direction - The authority necessary to ensure effective operation of a C4 system or activity. It includes the authority to direct and assign tasks to C4 operating elements and supervise the execution of those tasks; allocate and reallocate C4 systems or activity to accomplish the mission; and develop C4 technical standards, practices, methods, and procedures for performance and operations.

Communications Security - The protection resulting from all measures designed to deny an unauthorized person information of value that might be derived from the possession and study of telecommunications or to mislead unauthorized persons to their interpretations of the results of such possession and study. Also called COMSEC. Communications security includes:

1. Emission security - The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

2. Physical security - The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JCS Pub 1-02)

3. Transmission security - The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis.

4. Cryptosecurity - The component of communications security that results from the provision of technically sound crypto-systems and their proper use.

Computer Security - The protection resulting from all measures designed to prevent either deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of information in the computer system. COMSEC measures may be among those applied in achieving computer security.

Continental United States (CONUS) - United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. (JCS Pub 1-02)

Defense Information Infrastructure (DII) - The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users, across the range of military operations. It encompasses: (1) sustaining base, tactical, DOD-wide information systems, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapons systems, (2) the physical facilities used to collect, distribute, store, process, and display voice, data, and imagery; (3) the applications and data engineering tools, methods, and processes to build and maintain the software that allow Command and Control (C2), Intelligence, Surveillance, Reconnaissance, and Mission Support users to access and manipulate, organize, and digest proliferating quantities of information; (4) the standards and protocols that facilitate interconnection and interoperation among networks; and (5) the people and assets which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

Defense Information Systems Network (DISN) - Integrated network, centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services. Diverse Routing - Connectivity servicing the same facility, but routed over geographically separate circuits.

Dual Homing - The connection of a terminal so that it is served by either of two separate DISN centers.

End Office (EO) - An integral part of the DSN. Any EO switch provides switched call connections and all DSN service features, including MLPP to the users. The EO will provide long distance service by interconnection with DSN nodal switches. The EO will not serve as a tandem in the DSN but may connect to other EOs where direct traffic volume requires (Metro Calling Area).

Grade of Service (GOS) - The probability of call blockage expressed as a percentage of calls blocked. Grade P.05, for example, denotes that five calls of every 100 offered will probably fail to complete.

Host Nation Approval (HNA) - The approval given by a host nation for the operation of U.S.-owned C4 equipment within the host nation borders. This term is frequently misused by employing its usage when CA is the type approval being sought.

Host Nation Spectrum Supportability - The conceptual concurrence provided by the host nation in response to a formal request for information as to whether their national table of frequency allocations will support a proposed electronic emitter.

Internet - A term used to identify global communications and information sharing using existing commercial and other network infrastructure. Link or connectivity is provided by Internet Service Providers (ISP) and its use is commonly associated with personal computer users. A growing way to disseminate data over military networks.

Intranet - Similar in function to the Internet, but access is restricted to a specific group of computer users. Commonly used by corporations to manage data flow and restrict data access.

Joint Staff - The staff of the Chairman, Joint Chiefs of Staff, as provided for under the National Security Act of 1947, as amended by the DOD Reorganization Act of 1986.

Joint Worldwide Intelligence Communications System (JWICS) - The sensitive compartmented information component of the DISN. The primary mission of JWICS is to support the production and dissemination of intelligence to the entire intelligence community and is also used for command and control via its video teleconferencing application.

Management Control - The review, evaluation, coordination, and management actions necessary to fulfill the responsibilities of operational direction for a system or an activity.

Maximum Calling Area - A description of user calling privileges based on the destination of the call.

Metropolitan Calling Area - A community of interest having operational telecommunications needs in the local area.

Multilevel Precedence and Preemption - The capability to originate calls based on precedence and to preempt calls of lower precedence in the network.

Multimedia Conferencing - Comprised of the traditional VTC plus one or more of the following additional capabilities:

Applications and file sharing	File Transfer
Directory Access	Annotation
Embedded Icons	Capturing
Whiteboarding	

Netting - Manual interconnection of long-distance (originating at another switch) DSN calls with a local or long-distance commercial network. (See off-net and on-net calling.)

Nodal Switch - A tandem switch in the DSN that will connect multiple EOs, provide access to a variety of transmission media, route calls to other nodal switches, and provide network features such as MLPP. Nodal switches will be supervised by and interconnected to the DSN A/NM subsystem. The two types of nodal switches in the DSN are:

1. Multifunction Switch - This switch incorporates the combined functions of an SA switch and an EO switch. No physical division exists between the EO and SA functions within the MFS, but a logical division exists.
2. Stand Alone Switch - The SA switch functions solely as a tandem switch in the DSN.

Off-Net Calling - Calls placed over DSN extended to commercial telephone numbers.

On-Net Calling - Calls from commercial telephone numbers extended to the DSN network.

Precedence - Calling capability assigned to a DSN or DRSN user terminal. The five levels of precedence in ascending order are:

1. *ROUTINE* - Precedence designation applied to those official government communications which require rapid transmission by telephonic means but do not require preferential handling.
2. *PRIORITY* - Precedence reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of government operations.
3. *IMMEDIATE* - Precedence reserved generally for telephone calls pertaining to: (a) Situations which gravely affect the security of national and allied forces; (b) Reconstitution of forces in a post-attack period; (c) Intelligence essential to national security; (d) Conduct of diplomatic negotiations to reduce or limit the threat of war; (e) Implementation of Federal Government actions essential to national survival; (f) Situations which gravely affect the internal security of the United States; (g) Civil Defense actions concerning our population and their survival; (h) Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population; (i) Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

4. *FLASH* - Precedence reserved generally for telephone calls pertaining to: (a) Command and control of military forces essential to defense and retaliation; (b) Critical intelligence essential to national survival; (c) Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities; (d) Dissemination of critical civil alert information essential to national survival; (e) Continuity of Federal Government functions essential to national survival; (f) Fulfillment of critical United States internal security functions essential to national survival; (g) Catastrophic events of national or international significance.

5. *FLASH OVERRIDE* - Same as FLASH, capability available to (a) The President of the United States, Secretary of Defense and Joint Chiefs of Staff; (b) Commanders of combatant commands when declaring Defense Condition One or Defense Emergency; (c) CINCNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities the President may authorize. FLASH OVERRIDE cannot be preempted.

Preemption - The act of seizing telecommunications connectivity from a call of lower precedence to support calls of higher precedence.

Private Branch Exchange - A telephone exchange servicing a single organization or area where service requires connection to another telephone exchange for long-distance capabilities. A PBX, either manual or automatic (PABX), is customer premise equipment and is not an integral part of DSN. PBX and PABX are used interchangeably.

Special C2 Users - A special class of user who has access to the DSN for essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crisis, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among the President, Secretary of Defense, Chairman and other members of the Joint Chiefs of Staff, Chiefs of the Services, and the CINCs. Specifically, these special C2 users are identified through one or more Joint Staff, CINC, Service, or DOD agency validation processes. They are all DRSN subscribers as are the following identified subscribers of common user networks:

(1) Joint Staff - approved FLASH, FLASH OVERRIDE, or IMMEDIATE precedence origination capability.

(2) CINC or Service - approved IMMEDIATE or PRIORITY precedence origination capability.

(3) CINC - validated minimum essential circuits.

Stress Level - The military operating conditions under which DSN must function based on scenarios ranging from peacetime to massive nuclear attack.

STU-III family - One or more of the various models of the STU-III terminal (STU-III, STU-IIIA, STU-III cellular, STU-IIIR, etc.).

Tandem Switch - A switch or portion of a Multifunction switch that processes trunk group routing and connects only to other switches.

VTC - Electronic form of communication permitting face to face exchange of video and audio between two or among several participants simultaneously.

APPENDIX C

ACCESS TO THE DISN BY FOREIGN ORGANIZATIONS OR INDIVIDUALS

1. Access to the DISN by foreign organizations or individuals are governed by references A, E, and F, pg. A-1. The basic tenets for providing DISN services to foreign organizations or individuals require:

a. The connection assists in the fulfilling of broader US international agreements, including support of contingency or war plans.

b. It furthers specific goals (e.g. rationalization, standardization, and interoperability) consistent with current DOD goals.

c. The connection improves reliability of US military telecommunications by providing alternate routes or reserve capacity.

d. The connection is based on US military requirements, as in the case of active combined military operations.

e. The connection provides for telecommunications between US and foreign units or commands.

f. An exchange of service of equal value or reimbursement for the value of the service.

2. DISN services provided to foreign organizations or individuals will be formalized in an international agreement IAW ref. F, pg. A-1.

3. The concept for DISN support involving foreign organizations and individuals follows.

a. These categories receive DISN services without an international agreement.

(1) US personnel assigned to US billets in bilateral or combined organizations; e.g., representative to a Foreign Ministry of Defense, LNO to a combined headquarters, etc.

(2) US personnel assigned to US billets in international organizations, e.g. U.S. representative to NATO.

(3) US personnel dual-hatted; e.g. assigned to both a U.S. billet and a NATO billet.

(4) Foreign military/civilians assigned to foreign billets located in U.S. facilities under bilateral agreements or combined forces agreements; e.g. exchange officers.

b. These categories require Joint Staff or higher approval to receive DISN services.

(1) US personnel assigned to NATO or other defense organization billets, e.g. US military in a NATO billet at AFSOUTH.

(2) Non-US personnel assigned to NATO or other regional defense organization billets located in US facilities.

(3) Non-US personnel assigned to NATO or other regional defense organization billets.

c. HQ USEUCOM ECJ6 may approve emergency, non-permanent connections to the DISN for those categories in paragraph b during contingency operations. Any oral approvals will be put into writing as soon as possible. HQ USEUCOM approved contingency connections will terminate at the completion of the contingency operation, unless formalized by an international agreement IAW ref. F, pg. A-1.

4. Connections to the DISN will not parallel existing Allied communications systems, e.g. using the DISN to avoid toll charges, poor quality or traffic congestion on the allied network. DISN connections by allied organizations will not be designed to allow the allied organization to avoid comparable commercial service or to be in conflict with existing commercial services, laws, or regulations.

5. Allied connections to the DISN will only have ROUTINE precedence. They may not adversely effect the grade of service of the DISN.

6. Organizations requesting DISN service for allied organizations or personnel will forward the request through their chain of command to HQ USEUCOM, ECJ6-S, UNIT 30400 Box 1000, APO AE 09128, DSN 314-430-5564. See enclosure 1 of this appendix for sample memorandum.

7. USEUCOM ECJ6-S and ECLA will review the request to determine:

a. The legal, legislative, and funding authorities for a possible international agreement.

b. That the request satisfies the tenets in paragraph 1.

c. The approving authority.

8. Upon successful review in light of the above requirements, the requesting organization will be directed to begin exploratory discussions with the foreign entity to determine the basis for an international agreement. The requesting organization will also be directed to prepare a request for authority to negotiate an international agreement IAW ref. F, pg. A-1. The request package will consist of:

a. A cover memorandum stating the purpose for the request, and the US interests being served by the request.

b. A draft text of the proposed international agreement.

c. A technology assessment and control plan

d. A fiscal memorandum

e. A legal memorandum

ENCLOSURE 1 TO APPENDIX C

Sample DISN Foreign Access Request

MEMORANDUM FOR Director, Command, Control and Communications Systems, United States European Command, ATTN: ECJ6-S, Unit 30400, Box 1000, APO AE 09128

THRU: (appropriate intermediate headquarters)

SUBJECT: Request for connection to the DISN by (foreign organization or individual)

1. Reference:

a. CJCSI 6740.01, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations.

b. List any other correspondence on this matter and attach to request.

2. Request permission to begin non-binding exploratory discussions and to begin drafting an international agreement for (the subject connection).

3. Recommend validation of this connection as a candidate for an international agreement because it (state the US government interests being served).

4. For further information contact (Requesting agency point of contact and telephone number).

I. M. STRONG
COL, USA
Commanding

CF: DISA-EUR (EU2)

APPENDIX D

Defense Switched Network (DSN) Use Within Theater

1. General. The DSN is the primary voice switched network of the Department of Defense (DOD). It is designed to provide rapid, reliable, survivable, secure, and economic telecommunications for Command and Control (C2) users. For reasons of economy, the DSN also provides service to lower priority users on a noninterference basis. The DSN will be used only for official business and authorized purposes. DSN will be the first choice for all new and existing voice switched telecommunications requirements. As an official government network, it is subject to monitoring, and use of the DSN constitutes consent to have communications monitored for security and management purposes. Detailed policy for general voice requirements are covered in enclosure 1 to this appendix.

2. Secure Voice. The secure voice system (SVS) elements of the DSN will provide secure voice to authorized users in accordance with national security directives. The SVS includes C2 conferencing, general purpose conferencing, and the secure telephone unit III (STU-III) / secure telephone equipment (STE) family of equipment. Red Switches for the National Military Command Center (NMCC), NMCC Site R, and the primary command centers at the combatant commands along with other locations are included in the Defense Red Switch Network (DRSN). All regulations, directives, and policies of the DSN apply equally to the DRSN. Detailed policy for secure voice system is covered in enclosure 2 to this appendix.

3. Precedence. Precedence is a ranking assigned to a user terminal that indicates the degree of preference to be given in processing and protecting calls. Detailed policy for precedence is covered in enclosure 3 to this appendix.

4. Switched 56Kbps (SW56) Service. SW56 service is a capability for high-speed data service on a dial-up basis. It provides a capability for video teleconferencing, bulk file transfers, on-demand circuits for router networks, and high-speed facsimile. Demonstrated capabilities include video teleconferencing (VTC), high-speed fax (Group IV), digital secure voice, and computer and router data dialing. The DSN provides the transmission paths to conduct these digital applications, which can access the network via ISDN Basic Rate Interface (BRI) of propriety digital terminal devices. Ordering SW56 services to your site location will follow the current general guidelines contained in DISA Circular 310-130-1, Submission of Telecommunications Requests. A request for service (RFS) will be submitted by each site/location to the servicing telecommunications certification office (TCO), with additional addresses of DISA/D332, and DISA-Europe/EU22. Paragraph 401 of the RFS should read, “Orders issued to start (xx number) global switched 56 (SW56) service access lines." In paragraph 417 enter any narrative remarks which will assist to clarify the request for service as necessary and additionally request that all echo cancellers be inactivated. The area codes of 504 and 514 for Europe, 502 or 512 for CONUS and 508 or 518 for Southwest Asia are used for high-speed modem service, 9.6-56kbps.

ENCLOSURE 1 TO APPENDIX D

Policy For Non-Secure Voice Communications

1. General. DSN is the official Department of Defense (DOD) switched voice network and will be the preferred communications means for the special C2 and C2 user. It is the primary secure (STU-III family) communications means for non-tactical C2 users. DSN will be the user's first choice for communications, however, if DSN is not timely or if the called party does not have DSN access other commercial calling means may be used. The use of DSN is restricted to the official business and authorized purposes of the US Government.

2. Non-DOD Activities. Non-DOD activities may be granted access to the DSN network by the DOD when necessary for national security, when not in conflict with local ordinances of those activities, and which best serves national interest. If access is approved, DSN services will be provided on a cost-reimbursable basis. Request by non-DOD users should be satisfied by commercial means if the use is clearly not associated with the military mission of the DOD. Under no circumstances will access to DSN be granted simply as a cost-effective substitute for available commercial service. Requirements of non-DOD or non-governmental activities or agencies (e.g. DOD contractors, foreign embassies) are referred to the Office of the Secretary of Defense for approval with a recommendation from the Joint Staff except as listed in paragraph 2.a below.

a. Contractors:

(1) DSN may be used by US civilian contractor personnel in overseas areas when they are performing duties normally performed by DOD civilian or military personnel. DSN access may be provided to a foreign national contractor when validated by a US Government contracting officer and approved by the appropriate Component command. Only DSN calls directly related to and necessary for the accomplishment of contracted duties are permitted between overseas locations and CONUS or within an overseas theater.

(2) The requesting CINC, Chief of Service, or director of a Defense agency will validate the requirement, certify that contract documents contain guidance/restrictions, and is certified by a contracting officer to ensure that contractor use of DSN complies with established network management procedures. Request for approval will identify the contract termination date.

(3) Procedures for reviewing, monitoring, and controlling contractor access to DSN will be published in Service, command, or agency regulations. As a minimum, a review of contractor access to DSN will be conducted every 3 years and in conjunction with every renewal or period of performance extension of the contract.

(4) Approvals and contracts will state that DOD will have the right to terminate the service at any time and that DOD will not guarantee the quality or quantity of service to be supplied or be held liable for any discontinuance or failure of the service.

(5) DISA-EUR (EU2) will be provided copies of all contractor access requests, approvals, and terminations.

b. Foreign Governments - Foreign governments' activities may be granted access to the network by the DOD for national security and when not in conflict with existing agreements or local ordinances. This access will be initiated by and processed through the appropriate DOD sponsor IAW ref. F, pg. A-1.

c. Non-Appropriated Fund Activities (NAF) - DSN may be authorized for NAF activities to conduct command management functions dealing with appropriated funds matters. Requests should be forwarded through the appropriate component channels for approval and must be certified by the commander of the NAF activity as required for command management functions. Calls dealing with NAF business or functions other than command management will use the DSN on a cost reimbursable basis and if it does not impact the operational capabilities of the DSN. The USEUCOM component commands will institute procedures to revalidate NAF requirements every 2 years.

d. Labor Unions - Labor unions will not receive access to DSN nor routine authorization in contract documents. The basis for supporting a request to OSD will be a clearly operational, military related function. The Joint Staff, CINC, Military Service, Defense Agency concerned and DISA will be notified of command support for a request to OSD for labor union access to DSN.

e. Foreign Military Sale (FMS) - DSN service may be approved as part of an FMS arrangement. The use of DSN by DOD personnel assigned to non-US (foreign government adviser, UN, NATO, etc.) organizations must be validated or approved by USEUCOM ECJ6. If service is for non-US or non-DOD users, requirements will be submitted to OSD for approval.

f. Friendly Foreign Governments and Treaty Organizations - USEUCOM ECJ6 may authorize temporary use of DSN, at ROUTINE precedence, by personnel of friendly foreign governments or treaty organizations for the discussion of official US Government business with US personnel if such use will not reduce the GOS objectives outlined in this instruction. Components will ensure effective control of this use and will validate the service when other telecommunications facilities are unavailable. If the DSN access required by personnel of friendly foreign governments or treaty organizations becomes routine or becomes a formal requirement, the arrangement must be formalized by an international agreement IAW ref. F, pg. A-1.

3. Request for DSN Service. The procedures and format for requesting DSN service are listed in Appendix H.

Users who require a DSN phone in their *personal quarters* must have specific approval by an approval authority for that installation as designated by the component command. DSN phones approved for installation in personal quarters will not have local dialing access. Navy requests for DSN access in personal quarters must be validated IAW SECNAVINST 2305.11A.

ENCLOSURE 2 TO APPENDIX D

Policy for the Defense Red Switched Network

1. General.

a. The operational requirements have been validated for DRSN service to be provided to the NMCC, NMCC Site R, CINC Primary command centers, and component commands. Additionally, DRSN will provide the means to access tactical secure voice systems (i.e. KY-68 Digital Secure Voice Terminal (DSVT), AN/TTC-39 switches).

b. The DRSN is the primary network for secure conferencing and supports the majority of the Worldwide Secure Voice Conferencing System (WWSVCS) conferees. Other conferencing requirements will be accommodated by the DRSN on a non-interfering basis.

c. The DRSN is a dedicated secure network that is configured and managed by DISA. No automatic or dedicated trunking by other Red Switches is authorized. The DRSN network is monitored 24-hours-a-day, 7-days-a-week by a network management facility.

2. **Request for DRSN Service**. Requests for DRSN service, authority, and allocation of precedence is the same as the DSN. The procedures and format for requesting service are listed in Appendix H.

ENCLOSURE 3 TO APPENDIX D

Precedence Management For The Defense Switched Network (DSN)

1. General.

a. Precedence is a ranking assigned to a user terminal that indicates the degree of preference to be given in processing and protecting calls. The five levels of precedence in descending order are FLASH OVERRIDE, FLASH, IMMEDIATE, PRIORITY, and ROUTINE. Originators of a precedence call should use the lowest precedence level required to accomplish mission objectives.

b. Access to a level of precedence other than ROUTINE shall be determined only by mission requirements and shall not be used as a means of improving a grade of service above that provided to ROUTINE users. Any change in the assignment of precedence levels must be reviewed by DISA to ascertain the network impact and to size the DSN and DRSN architecture to accommodate the change.

2. Policy.

a. FLASH OVERRIDE, FLASH, IMMEDIATE, and PRIORITY precedences are intensively managed at the Joint Staff and Commander-in-Chief (CINC) levels.

b. ROUTINE is the standard precedence assigned to DSN and DRSN user terminals.

c. DSN and DRSN users demanding higher precedence must ensure their request is based solely on operational requirements.

3. Procedures.

a. Requests for higher precedence.

(1) Precedence requests must comply with the following:

(a) Joint Uniform Telephone Communications Precedence System guidelines.

(b) Paragraphs 17 and 18 of enclosure A to ref. E, pg. A-1.

(c) Approved Component precedence templates.

(2) Any deviations from paragraph 3.a.(1) above must be presented to the respective approval authority (see paragraph 3.a.(4) below) with justification for adjudication.

(3) The Joint Staff approves all FLASH OVERRIDE and FLASH precedence requests worldwide.

(4) The Commander-in-Chief, European Command (CINCEUR) approves all IMMEDIATE, and PRIORITY precedence requests and validates all FLASH OVERRIDE and FLASH precedence requests in Theater.

(a) CINCEUR further delegates the USEUCOM ECJ6 as the approval authority for IMMEDIATE and PRIORITY precedence requests and the validating authority for FLASH OVERRIDE and FLASH precedence requests over the DSN and DRSN.

(b) The USEUCOM ECJ6 further delegates the Component Commanders as the validating authority for IMMEDIATE and PRIORITY precedence requests over the DSN and DRSN.

b. Format of Requests. All requests will follow the format attached at enclosure 1 of appendix H.

c. Routing of Requests.

(1) All requests for precedence upgrade will be forwarded to the appropriate office indicated above after validation by the chief of the requesting agency. The appropriate office is the Component command providing the switch at the agency location. For example, the USNAVEUR Personnel Services Division (PSD) at Patch Barracks, Germany, requests precedence upgrade to PRIORITY through CINCUSNAVEUR N-6 to USAREUR since the Army provides the switch at Patch Barracks.

(2) All requests for precedence upgrade from designated joint or combined task forces will also be reviewed by ECJ6-O for compliance with appropriate deployment orders.

4. USEUCOM ECJ6 will maintain a database of all approved precedence users in theater. In addition, a separate database of all contingency, short-notice precedence upgrades will be maintained. Any precedence assignments not contained in the permanent or temporary databases will be removed from the switch by the owning component immediately upon discovery.

5. All approved precedence assignments will be revalidated at least biennially. USEUCOM ECJ6 will provide a list of expiring precedence approvals to the component action offices NLT 1 Mar. These expiring precedence approvals will be removed from the theater databases NLT 1 Oct unless revalidation messages are received prior to 1 Oct.

6. Upon receipt of the Joint Staff or USEUCOM approval, as required, the request for service (RFS), telecommunications service request (TSR), and telecommunications service order (TSO) actions must be completed prior to the formal implementation of a precedence upgrade on the DSN switch (per pg. A-1, ref. K). Upon receipt of required authorization/funding documentation, DISA-EUR will release a switch revision message (SRM) to install precedence authorizations and/or upgrades to servicing switches. Exceptions to this rule will require USEUCOM ECJ6 or the appropriate component command validating authority approval.

APPENDIX E

Video Teleconferencing

1. General. Video teleconference is an evolving electronic form of communication becoming prevalent for both tactical and strategic requirements in theater. To ensure that USEUCOM and all its Component commands and supporting agencies can achieve interoperability, all VTC systems (tactical and strategic) in theater must be capable of using DOD standards. All VTC systems operated in USEUCOM will use the DOD standards specified in the current Joint Technical Architecture. Enclosure 1 to Appendix E outlines a summary of the minimum standards for VTC.

2. Secure Conferencing. All multi-point secure conferencing will be done using only approved and accredited hubs. Point to point conferencing will be conducted IAW paragraph 3.b below.

3. The VTC architecture for USEUCOM has five distinct operational technical layers (i.e. Unclassified, Secret, Top Secret, NATO, and SCI). Currently, VTC users are prohibited from creating connections that cross layer boundaries unless all security and/or technical requirements are met and the appropriate network manager has granted written authorization. The long term vision for USEUCOM remains an evolving technical standard that will allow seamless interconnection between layers.

a. The Joint Worldwide Intelligence Communications System (JWICS) has a VTC sub-network that allows VTC participants to conduct conferences at the Top Secret/SCI level. JWICS provides VTC capability between CINCEUR and the National Command Authority. The data portion of the Joint Deployable Intelligence Support System (JDISS) also supports TCP/IP based desktop VTC and multicast transmission over the JDISS network. The VTC portion of JWICS operates at 384KB (medium) or 512KB (high) data rate and is protected by KG-194 COMSEC devices. Configuration management and technical standards are coordinated through ECJ2 to the Defense Intelligence Agency.

b. The DISN Video Services - Global (DVS-G) hub serves as the theater's primary multi-point control unit to support common-user tactical and strategic multi-point VTCs up to the Top Secret Collateral level. It is part of the DISN global common-user VTC (narrowband) and will serve all levels of command. This network supports a variety of equipment ranging from the dedicated VTC suites, roll-around VTC equipment, to VTC equipment installed on personal computers. The DISN global VTC network serves users in point-to-point or multi-point modes. Primary connectivity is through dial-up ISDN and Switched 56 (SW56) DSN service. Users are required to register their sites with the hub prior to use. Selected users may submit a Request for Service for dedicated bandwidth when operational needs and costs warrant. Multi-point conferences will be established by dialing into designated theater VTC hub facilities. The hub will provide the bridge that permits multi-point video/audio conferences. The minimum data rate for common user VTC is 112/128 Kbps. This system will be protected by KG-84/KIV-7 **or equivalent**

COMSEC devices when operating in the classified mode. Unclassified conferences may be established. The Video Information Exchange System (VIXS), the Navy system operating in theater, is capable of both Secret and TS/SCI levels. All common user VTCs will comply with the H.320 technical standard. Information for the site registration form required for access to the theater hub is at enclosure 2.

c. Low data rate VTCs using existing office or tactical telephone systems for connectivity, are usually add-on boxes to existing telephone instruments. They exchange data at low data rates typically up to 56 Kbps. These systems will be protected by the appropriate COMSEC device for the user telephone equipment (for example: STU-III, KY-68). Because these systems operate at low data rates their ability to handle real-time movement is extremely limited. Low-rate systems will comply with the H.324 standard. This standard will not be supported for multi-point VTCs in this theater.

d. Internet Protocol (IP)-based VTC or multimedia applications use the existing data networks, such as SIPRNET/ NIPRNET, and are connected to local and wide area networks to exchange data. These high-data rate systems operate at up to 10 Mbps. Because this technology is continually emerging, the standards and protocols for these types of systems are not yet finalized. Due to the significant affect these applications have on the data networks, those systems operating across wide area networks will only be procured, installed, and implemented when validated by ECJ6-S and technically approved by DISA-EUR. Organizations implementing TCP/IP-based VTC networks for use within a local area network will establish management controls to prevent entry into the DISN. No organization subject to this directive will implement any video application that uses “multi-cast” technology. Waivers may be requested through ECJ6-S.

e. Standardized Tactical Entry Point (STEP) will provide VTC connectivity to the theater DVS-G hub for tactical VTC requirements. Tactical VTC user equipment will meet the technical standards, minimum data rates and security requirements outlined in para. 3 (b). Tactical VTC user equipment will be registered with the DVS-G hub prior to deployment. See enclosures 2 and 3 for the documents necessary to register equipment. Tactical VTC users will be able to make secure and non-secure point-to-point and multi-point connections through the theater DVS-G hub. There will be no direct point-to-point VTC connections between deployed and strategic users. All tactical to strategic connections through the STEP must utilize the DVS-G hub.

f. All changes to the configuration of the USEUCOM AOR VTC architecture will be submitted to the theater voice configuration control board.

ENCLOSURE 1 TO APPENDIX E

Tactical and Strategic Minimum Video Teleconferencing Standards

	Common User (narrowband) VTC H.320 (112/128 Kbps)	**Low data rate VTC H.324 (9.6-56Kbps)**	**IP based VTC H.323 (Requires USEUCOM ECJ6-S and DISA-EUR approval for WAN use)**
Connectivity	ISDN/SW56	POTS/DSVT/STU-III	Ethernet
Video	H.261	H.263	H.263
Audio	G.711, G.722, G.728	G.723	G.711, G.722,G.723,G.728
Encryption	H.233,H.234	H.233,H.234	TBD
Transmission Multiplexing	H.221	H.223	H.222
Signaling	H.230,H.242	H.245	H.230,H.245
Multi-point Control	H.243	N/A	N/A
Data/Telematic Protocols	T.120	T.120	T.120

ENCLOSURE 2 TO APPENDIX E

VTC Site Registration

The VTC Site Registration Form is available on DISA-EUR unclassified web page at url: http://www.eur.disa.mil/disaeur/dii/vtc/vtc.htm.

APPENDIX F

Data Networks

1. General. Use of government computer networks and systems shall be for official use and authorized purposes only. Official uses are those uses directly related to the discharge of official duties and other uses as defined in reference K, section 2-301a(1). Authorized purposes are those uses expressly permitted by reference K, section 2-301a(2), which fall outside the scope of "official use." Users must also comply with any policies or procedures associated with specific computer systems. Use of government computer networks and systems is subject to monitoring. Activity on computer networks, government or otherwise, is not anonymous and does not provide any expectation of privacy.

2. The DISN-E will be the primary data backbone network for USEUCOM. Deviations from this policy will require validation by ECJ6 and approval by the Theater Data Configuration Control Board.

a. A limited number of waivers to this policy were granted and are documented in the HQ USEUCOM European Unclassified IP Router Network Memorandum, dated 9 Dec 94, and the HQ USEUCOM Secret IP Router Topology Agreement, dated 1 Feb 95. They were granted in recognition of specific mission requirements and the related economies of effort. These agreements will be periodically reviewed by the Theater Data CCB to examine the feasibility of further migrating these systems into the DISN.

b. Unless specifically identified in those agreements referenced in paragraph 2.a., components and agencies will use the DISN for long-haul data communications requirements. DISA will provide requesting components and agencies appropriate technical and cost analysis for long-haul data transfer options.

3. Service components and agencies will utilize existing DISN communication servers where available. Development and use of separate (non-DISN) communication services will only be allowed under extraordinary circumstances and will require approval by the Theater Data CCB.

4. HQ USEUCOM has validation authority for all requests for backbone or long-haul data services.

5. DISA-Europe will have network monitoring and control of its DISN data network resources with real time visibility into component and agency resources. DOD users who are serviced by a component will be monitored to ensure reliable data service is being provided in accordance with DISA Circulars 310-130-2, Defense Communications System Management Thresholds and Performance Objectives, 310-55-1, Status and Reporting for the Defense Communications Systems, and DISA-Europe Supplement 2 to DISA Circular 310-55-1, Status Reporting for the DCS European Area.

6. Use of DISN Internet services must be work-related and includes all communications determined to be in the interest of the Federal Government. Such use should be appropriate in its

frequency and duration, and related to assigned tasks. Examples of authorized use include using the Internet to:

a. Improve professional or personal skills as part of a formal academic education or military or civilian professional development program (when approved by an immediate supervisor).

b. Obtain or exchange information that enhances the professional skills of DOD employees and benefits the DOD and job performance within the DOD.

c. Obtain or exchange information to support DOD missions.

7. Government computers may be used to access the Internet for incidental personal purposes (see Appendix G).

APPENDIX G

Health, Morale, And Welfare (HMW) Use Of The DISN

1. General. Government networks exist to support the official requirements of the warfighter, including emergency communications. Use of the DISN for HMW communications will be on a space available basis. HMW traffic loading will not be a basis for expansion of government networks. Use of the DISN constitutes consent to have all communications monitored for security and management purposes. Components will establish policy and procedures to allow limited space available access to government operated unclassified voice and data networks for:

a. Brief communications between deployed members and their immediate families for family support and morale purposes. For the purposes of this policy, a deployed member is defined as a military member or DOD employee on extended official duty away from their primary residence in an unaccompanied status.

(1) Unit/element commanders will establish policy to control morale voice and data communications accommodating operational needs, and IAW local and host nation laws and requirements. This policy will specify the time of day such communications are allowed, duration, and frequency.

(2) Normally morale voice communications should be made during the military member's/DOD employee's off-duty hours for no more than 15 minutes twice a week per individual.

(3) Morale communications will be at routine precedence from phones and/or terminal devices under control of the local commander.

(4) USEUCOM Component Commanders will designate remote locations for HMW communications in writing.

(5) Local commanders may establish temporary user and communication server accounts on unclassified networks for entitled dependents to facilitate access at home base family support activities. Entitled dependents are those whose sponsors are deployed to remote locations. If temporary user/server accounts are established, local commanders must establish safeguards to protect the network from deliberate or accidental degradation by a temporary user.

b. Brief communications by military members and DOD employees during official travel to notify family members of official transportation or schedule changes.

c. Reasonable personal communications for the purpose of arranging such things as auto repairs, home repairs, child care, or medical appointments from the military member's or DOD employee's workplace providing that such communications:

(1) Would not reflect adversely on the DOD such as using the DISN for uses involving pornography, racism, chain letters, unofficial advertising or solicitation, inappropriate

handling of classified information, soliciting or selling except on authorized bulletin boards and other uses that are incompatible with public service.

(2) Serve a legitimate public interest, such as enabling the military member or DOD employee to stay at their duty rather than requiring them to depart the duty area to use commercial systems, or improving the morale of military members stationed away from home for extended periods.

(3) Do not create significant additional cost to the DOD. This concerns calls that incur a long distance charge because they exceed the authorized local commercial calling area of the DSN switch (see off-netting in basic policies).

(4) Are of reasonable duration and frequency, such as a brief Internet connection or telephone call and made whenever possible during the military member's or employee's personal time, such as lunch time or authorized breaks.

(5) Do not adversely affect the performance of the organization or the official duties of the military member or DOD employee.

(6) Do not overburden the government systems.

2. Those individuals wishing routine or frequent access to the Internet for personal use must subscribe to a commercial access provider directly.

3. Commanders at all levels will employ controls to protect government information and communications resources from fraud, waste, abuse, mismanagement, or misappropriation.

APPENDIX H

Procedures For Requesting Validation of DISN Service

1. Purpose. Provides procedures for requesting DISN service validation. The format contained in enclosure 1 will be used for precedence requests for DSN and DRSN service. Other requests (e.g., switching changes, non-DOD customers) may be processed with unformatted memorandums or messages but must include the same basic information.

2. Applicability. These procedures apply to HQ USEUCOM, USEUCOM Components, and DOD Agencies operating in the USEUCOM AOR. All activities will request service validation through their chain of command from USEUCOM ECJ6 or the appropriate designated component approval authority per local procedures. Non-DOD agency requests sponsored by DOD components will also comply with these procedures. Non-DOD requests will be forwarded through ECJ6 through the Joint Staff to ASD(C3I) for consideration. HQ USEUCOM staff elements will request DISN services validation directly from ECJ6.

3. General.

a. Requests for DISN service. Requirements must be fully documented and justified. Component commands and DOD Agencies may tailor the format for requests that they approve. Future requirements (those appropriate for DISN Project Plans) should be provided to DISA and the Services.

b. Activities having validation or approval authority will ensure that requirements comply with this instruction. Specifically:

(1) Requests for DISN services support legitimate mission requirements.

(2) Precedence capabilities are justified in terms of explicit mission need and negative impact if the request is disapproved. Network status provided by DISA will be reviewed to determine what capabilities currently exist, whether current access in service is fully used, and the impact of requested service on the grade of service for the requesting location. Precedence requests from HQ USEUCOM staff elements require flag officer validation.

(3) Requirements for Red Switch connectivity or tandeming are justified and cannot be met by STU-III terminals. HQ USEUCOM requests for DRSN service require flag officer validation.

(4) Requirements that affect other component commands, Services, or Defense agencies have been coordinated.

(5) Tradeoffs are provided for new or increased levels of service or capabilities as required.

(6) Appropriate restoration priorities are identified.

c. Requirements Processing.

(1) Routine requirements will be processed by DISA-Europe after proper validation of the request. DISA-Europe processing time for routine requirements is 21 calendar days while systems control facilities have 15 calendar days.

(2) Validated urgent requirements will be processed immediately by DISA-Europe. "Urgent" is designated only for telecommunications services within the purview of the U.S. government. It does not have any effect on the procurement of commercially leased services. Government agencies will expedite processing of all urgent requirements. However, once the document is forwarded to the national allied long line agency NALLAs/PTTs (commercial services), it is a normal requirement.

(a) Urgent requirements are justified if lack of service:

- Seriously degrades mission performance and operations in direct support of national security preparedness
- Seriously degrades or impairs the execution of "real world" military plans or intelligence operations
- Seriously degrades or impairs the ability of the United States to maintain favorable foreign relations

(b) All urgent TSRs must contain sufficient justification and be certified by the validating authority for the component command. Validating authorities for European urgent requirements will be USAFE/SC, USAREUR/AEAIM, CINCUSNAVEUR/N6, or USEUCOM/ECJ6. Alternates may be designated by the components but will not be delegated below the O-6 level.

(c) All urgent TSRs will contain the following information: "If service date cannot be met, service is required as soon thereafter as possible. Do not provide service after (date)."

(3) Emergency Requirements. Emergency requirements are identified by the European public telephone and telegraph providers as circuits requiring "Exceptional Provisioning." Exceptional provisioning may be considered if any of the following conditions apply:

- Heightened tension (not amounting to a state of alert);
- Major incidents (calamities, natural disasters, catastrophes, and similar events);
- An unforeseen urgent exceptional requirement where the use of normal procedure would seriously hamper the accomplishment of the mission.

(a) Requests for exceptional provisioning must be in memorandum format, certified and signed by a general officer or civilian equivalent. Certification authority for exceptional provisioning cannot be delegated.

(b) All emergency TSRs must contain sufficient justification in item 417 to meet the aforementioned criteria. In addition, USEUCOM ECJ6-S must validate all emergency circuit requirements in the European theater. Authorization for use of exceptional provisioning is limited to the USEUCOM ECCC (USCINCEUR), ECDC (DCINC), ECCS (Chief of Staff) and ECJ-6.

(c) Response times for exceptional provisioning are listed in Table H-1.

d. Requests from activities outside the Department of Defense will be forwarded through the ECJ6 to the Joint Staff to ASD(C3I) for consideration.

e. Validation requests must indicate source of funding for the DISN service.

Response Times for Exceptional Provisioning of European Circuits
TABLE H-1

Exceptional Provisioning Catagories IAW ALLA Compendium	Heightened Tensions	Other Than Heightened Tensions	Unforseen Urgent Exceptions
Country	24 Hr (min)	24 - 96 Hr	30 Days or As Soon As Possible
Belgium[1]	X	X	X
Denmark[2]	X	X	-
France[3]	X	X	-
Germany	X	X	< 30 days
Greece	X	-	-
Italy	X	X	< 30 days
Luxembourg	X	-	X
Netherlands[4]	-	X	X
Norway[5]	-	-	-
Portugal	X	-	X
Turkey	X	-	< 30 days
United Kingdom	X	X	X

Notes:
1. Belgium code word “exceptional” required; must appear in Circuit Demand Line Alpha (for telephonic requests, individual authorized to call must be known in advance)
2. Requester may talk to PTT directly
3. Other than exceptional provisioning dealt with during normal working hours
4. Within 72 Hrs
5. All demands acted upon as soon as possible

ENCLOSURE 1 TO APPENDIX H

Validation Request Format

Request Format. The following message format will be used when requesting DISN service validation/approval from ECJ6:

FROM: (Originating Activity)

TO: USCINCEUR VAIHINGEN GE//ECJ6S//*

(* or activity with requisite approval authority)

INFO: (appropriate military department or agency requiring and funding the capability)

Subordinate command validating authority (example HQ USAFE RAMSTEIN AB GE//SCM// and/or others as required).

(DISA-EUR VAIHINGEN GE//EU/EU2/EU3// will be an information addressee on all requests.)

(If approval authority is below the HQ USEUCOM level, information addressees will consist of affected commands or agencies.)

UNCLAS or appropriate classification

MSGID/GENADMIN/as appropriate per MTF//

REF/as appropriate per MTF//

AMPN/as appropriate per MTF//

NARR/as appropriate per MTF//

REPLY/as appropriate per MTF//

RMKS/SUBJECT: (identify location or activity requesting service) request for DISN services validation. (example USAFE REQUEST FOR DSN PRECEDENCE AT RAF MILDENHALL)//

1. Description of required capability (concise narrative description, e.g. The commander, 3rd Air Force, requires immediate/CONUS precedence for coordination with higher headquarters and subordinate command. The commander, 3rd Air Force, is responsible for operational command and control for all air support missions within the 3rd Air Force area of responsibility. Precedence is required to provide timely and reliable communications in support of operational requirements).

a. Complete identification of the requirement (e.g., type of change, deletion, or addition including circuit or equipment quantities, configurations, sequence or identification numbers).

b. Identification of maximum calling areas and expected frequency and duration of calls, data transmissions, or duration of service. Information may also be expressed in terms of Erlangs of traffic.

c. Number of extensions required. Indicate if extensions are to be located in geographically separate locations that will require long-haul connectivity to servicing switch.

d. Terminating Equipment; e.g., Type, Brand, Model of PBX, facsimile, data terminal/modem, VTC studio terminal equipment, EAC, STU-III.

e. Tradeoff (identify by sequence number, CCSD, precedence, Joint Staff approval number, or other pertinent data).

f. Start date (if short notice, give justification and mission impact of delay).

g. Unit, title, and geographic location of requesting agency.

h. DISA or Joint Staff waivers in effect.

i. Servicing switch (EO, MFS) if applicable.

j. Precedence/Calling Area requested.

k. Location (geographic and physical).

l. Restoration priority or TSP.

2. Justification.

a. Present DISN capabilities and why they are inadequate.

b. Detailed description of the mission directly supported by the requirement or the mission change that generated the requirement and mission impact if disapproved.

c. Local commander(s) approval and point of contact, with telephone number.

d. Identification of DISA-EUR representative who provided coordination and network impact assessment office code, and phone number or why DISA was not contacted.

e. Identification of expected yearly cost, source of funds, and funding POC.

f. Certification by component commander (HQ USEUCOM flag officer for staff elements) or designated representative that the requirement is in compliance with ref. E, pg. A-1. and precedence templates. (Provide name and telephone number).

g. Non-DOD activities will not be connected to the DSN/DRSN without:

(1) Technical and security approval by DISA.

(2) Recommendation of a DOD sponsor.

(3) Concurrence of the Joint Staff.

(4) Validation by ECJ6.

(5) Approval of OSD.

h. Explanation if no tradeoff is provided.

3. Component command, staff element, or agency point of contact (name, office symbol, DSN, and commercial phone numbers).

(NOTE: Streamlined procedures authorized for deactivation or cancellation of DISN service)

APPENDIX I

Defense Information System Network-Europe (DISN-E) Configuration Management

1. Purpose. Provides policy and procedures for configuration management of the Defense Information System Network-Europe (DISN-E). It provides guidance for processing configuration changes and standardization criteria for implementing configuration management within the HQ USEUCOM Area of Responsibility (AOR).

2. Applicability. This policy provides guidance to U.S. European Command, U.S. European Components, DISA-Europe functional managers and U.S. Federal Government contractors working in the European Theater.

3. General. As a sub-element of the Defense Information Infrastructure (DII), DISN-E is part of the DOD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. Therefore, for purposes of this configuration management policy, the following networks/systems are considered a part of DISN-E:

- Voice Switched Services (Unclas/Clas)
- Integrated Protocol Router Networks (IP Router-Unclas/Clas)
- Video Teleconferencing (VTC)
- Joint Worldwide Intelligence Communication Systems (JWICS)
- Automatic Digital Network (AUTODIN)
- Integrated Digital Network Exchange (IDNX)
- Commercial Satellite Communications Initiative (CSCI)
- Bosnia Command & Control Augmentation (BC2A)
- Standardized Tactical Entry Point (STEP)
- Digital European Backbone (DEB)
- Leased Transmission Media (Point-to-Point)
- DCS Mediterranean Improvement Program (DMIP)
- Defense Satellite Communications System (DSCS)
- Digital Patch & Access System (DPAS)
- High Frequency (HF)
- Transmission Monitoring & Control System (TRAMCON)
- Asynchronous Transfer Mode (ATM) Backbone
- Integrated Services Digital Network (ISDN=SW56)
- Global Broadcast System (GBS)

4. Configuration Management. Configuration management is defined as a discipline applying technical and administrative direction and records management over the life cycle of items to

identify and document the functional and physical characteristics of configuration items. This includes controlling changes to configuration items and their related documentation; recording and reporting information needed to manage configuration items effectively, including the status of proposed changes and implementation status of approved changes; and auditing configuration items to verify conformance to specifications, drawings, interface control documents, and other contract requirements. All changes to the configuration of the DISN-Europe including new connections, modifications, reconfigurations, etc., will be submitted to the appropriate TCCB for approval prior to implementation IAW ref. I. Changes to the USAREUR common user data network (CUDN) or the secure data network (SDN) will also be submitted to the Theater Data Configuration Control Board for approval. Base-level communications reconfigurations that require DISN resources (voice, data, transmission), affect security classification, or affect the current/evolving DISN topology will require approval through the appropriate TCCB.

5. Theater Configuration Control Boards (TCCBs). Configuration management for DISN-E will be implemented through the use of Theater Configuration Control Boards (TCCB). The TCCBs will ensure the functional managers approve all changes being made to the DISN-E networks/systems and ensure effective and efficient utilization of resources throughout each of the networks. There will be three TCCBs established to manage DISN-E. TCCBs will normally meet on a monthly basis. However, the Chairperson of each Board reserves the right to convene meetings, as required. The meetings will be held in conference, via teleconference or VTC. The three functional area TCCBs with sub-elements are:

- Voice TCCB (DSN, DRSN, VTC, ISDN (SW56))
- Data TCCB (Router (Clas/Unclas), JWICS, AUTODIN)
- Transmission TCCB (DEB, IDNX, TRAMCON, DSCS, DMS, DMIP, CSCI, STEP, DPAS, HF, ATM)

Each TCCB will consist of, but not be limited to, the following membership:

- USEUCOM J6 representative
- DISA-Europe functional manager
- EU5 representative
- Representatives from each of the Component commands
- HQ DISA/D3 representative
- JEIO engineer
- EU8 representative

The DISA-Europe functional manager(s) will act as Chairperson of each Board with a division representative acting as the Secretariat. If required to resolve technical issues, an advisory group or technical specialist can be called at any time by the DISA-Europe TCCB Chairperson. The members of the European TCCB will have the opportunity to concur/non-concur with requested network changes. USEUCOM J6 designated representative has the responsibility of validating and approving DISN-E requirements. However, the European TCCB Chairpersons retain the authority to approve/disapprove DISN-E connections ensuring they meet validated operational requirements and connections meet all technical, security and interoperability requirements.

6. Change Control Documents. There will be two documents recognized as change control documents for DISN-E, Engineering Change Proposal (ECP) and the Telecommunications Service Request (TSR). Utilizing these documents will ensure timely network reconfigurations and accurate documentation for tracking network (re)configurations. This applies whether the systems are being developed or consist of Commercial-Off-The-Shelf (COTS) products. These documents will be utilized by HQ DISA, DISA-Europe functional managers, European Components, government contractors responsible for operations and maintenance (O&M) of DISN-E, and any Federal agency requesting services of the DISN-E. The originator will submit changes a minimum of 30-45 days prior to network reconfigurations. This will allow the appropriate functional managers and European TCCB members to review, plan, and implement the requested change(s).

The change control documents are:

a. Engineering Change Proposal (ECP) -DD1693 (Short Form): This document will be used by planning personnel who determine hardware, software or transmission bandwidth changes are necessary to allow the network(s) to operate at an optimal level. This document will be used regardless of cost/no-cost to a contract. Examples of changes include hardware upgrade, installation of cards, software upgrades, installation/de-installation of nodes. Under Configuration Management guidelines, there are 3 classes of ECP(s) that are identified in this document. These classes will be the following:

- Class I. Class I ECPs modify settings or configurations to DISN inter-theater gateway nodes, transmission, timing and synchronization CI(s) or requires DISA to expend funds. This class determination will be made by DISA-Europe functional managers. This type of ECP will be submitted to HQ DISA personnel for coordination and funding approval. Therefore, HQ DISA managers will be held responsible for coordinating their requirements with the appropriate HQ DISA divisions for approval (i.e. funding).

- Class II. Class II ECP(s) modify settings or configurations to the DISN-E intra-theater nodes, transmission, and timing and synchronization CI(s). These ECP(s) will be reviewed by the appropriate European TCCB and will be approved by the respective TCCB Chairperson(s), after technical/funding issues have been resolved, if any exist.

- Class III. Class III ECP(s) modify settings to DISN-E nodes, transmission, and/or end instrumentation that affect the users on posts, bases, camps, and stations. In most cases, these are actions that will be approved at the base level, however, if the change effects the DISN-E network then the Class III changes can result in succeeding Class II and Class I change recommendations. If base-level planners are not able to determine effects on the DISN-E, then they are required to coordinate these changes with DISA-Europe functional managers.

b. TSR/TSO Actions: The TSR and TSO are recognized as change control documents for activating/deactivating circuits and usually, follow a request to add, delete, or change

hardware/software within a network node. If this is not the case, the TSR/TSO will stand alone as a service activator change control document.

If the originator or the network functional manager determines there are multiple network changes or one network change causes other network changes to occur, then the originator shall do one of the following:

- Submit multiple forms (ECPs/TSRs) for each change required. This will be done if the originator is responsible for other nodes that are affected by the originator's requested change.

- On the ECP form, the originator will make a notation for DISA-Europe personnel so the necessary documentation can be submitted to allow the other changes to occur in sequence with the original request.

- On the TSR/TSO form, the approved ECP will be referenced in the Reference section.

7. Completion Reports: The Circuit Management Office (CMO)/Circuit Control Office (CCO) will submit a completion report to document the completion of a network change. In a fee-for-service environment, Completion Reports are mandatory for network equipment and configuration verification. In the technical environment, these Completion Reports enable functional managers, technicians and engineers the ability to assist customers with determining new requirements, technical issues, and billing issues.